99

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/749,142	12/27/2000	Thomas Wille	DE000002	4761

24738 7590 09/30/2005

PHILIPS ELECTRONICS NORTH AMERICA CORPORATION
INTELLECTUAL PROPERTY & STANDARDS
1109 MCKAY DRIVE, M/S-41SJ
SAN JOSE, CA 95131

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/30/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/749,142	WILLE ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-4 and 6-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-4 and 6-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 December 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment submitted in connection with the RCE filed 07/14/2005. Claims 2-4, 7, 10-14 have been amended; claims 15-28 have been added.

Response to Arguments

2. Applicant's arguments with respect to claims 2 and 10 have been considered but are not persuasive.

In response to applicant's argument that the Office Action does not describe how Patarin's process would be modified to include Jahnich dummy program (p. 11, 2nd paragraph), the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

Applicant argues that Jahnich does not disclose the limitation of using the dummy operations as part of a superimposition of consumption characteristics so that reconstruction of the consumption characteristics associated with performing the cryptographic operation is impeded (p. 11, 3rd paragraph). Jahnich discloses that the consumption characteristics generated by the dummy operation is part of the

consumption characteristics of the smart card when executing both the cryptographic operation and the dummy operation so that reconstruction of the consumption characteristics associated with performing the cryptographic operation is impeded (col. 6, lines 29-52).

Applicant argues that the Office Action does not set forth any sufficient suggestion or teaching in Tan, Jahnich or Patarin to support the conclusion that it would be obvious to modify Pantarin process to use the random control of Tan (p. 11, last paragraph). The discussion of Tan teaching and the reason to combine the references were cited in paragraph 5, pages 4-5, of the previous Office Action.

Priority

3. A translation of the foreign application is required in reply to this action for the purpose of determining the Applicant's right to rely on the foreign filing date.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claim 28 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had

possession of the claimed invention. Claim 28 recites the limitation "temperature, or other indirect radiation" in line 2. The specification as originally filed discloses that the consumption characteristics are based on current/power consumptions (page 3, lines 10-24; page 4, lines 7-11); however, it does not disclose that the consumption characteristics are based on temperature or other forms of indirect radiation.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

7. Claims 2, 4, 7, 10-13, 15-18, 20-24 and 28 are rejected under 35 U.S.C. 102(e) as being anticipated by Ugon et al (6,839,849). Applicant cannot rely upon the foreign

priority papers to overcome this rejection because a translation of said papers has not been made of record in accordance with 37 CFR 1.55. See MPEP § 201.15.

Regarding claims 2, 4, 7, 10-13, 15-18, 20-24 and 28, Ugon discloses a device comprising a CPU and a co-processor which perform cryptographic operations and dummy operations simultaneously and in parallel. Ugon also discloses that consumption characteristics of the device being a superimposition of consumption characteristics associated with performing both cryptographic operations and dummy operations so that reconstruction of the consumption characteristics associated with performing the cryptographic operation is impeded (Abstract; fig. 2; col. 3, lines 13-15; col. 8, lines 5-15; col. 9, lines 13-28; col. 10, line 56 – col. 11, line 3).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 3, 6, 8, 14 and 25-26 rejected under 35 U.S.C. 103(a) as being unpatentable over Ugon as applied to claims 2, 13 and 15, above, and further in view of Tan (6,490,353).

Regarding claims 3, 6 and 25-26, Ugon does not disclose that the selection of a processor to perform a cryptographic operation is randomly controlled. Tan discloses

that that the selection of a processor to perform a certain cryptographic operation is randomly controlled (col. 3, lines 60-64; col. 6, lines 6-12). It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the device of Ugon such that the selection of a processor to perform a cryptographic operation is randomly controlled, as taught by Tan, so that security could further be enhanced.

Regarding claims 8 and 14, Ugon does not disclose that the split-up of the cryptographic operation is randomly controlled. Tan discloses that data to be encrypted is segmented into blocks and that the size of each data block and length of the corresponding encryption key for each block are randomly selected (col. 3, lines 8-42); the selection of the block size and the key length meet the limitation of splitting up a cryptographic operation. It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the Ugon method such that the split-up of the cryptographic operation is randomly controlled, as taught by Tan, to increase the degree of difficulty in attacking the encryption system.

10. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ugon as applied to claim 7 above. Ugon discloses that the device performs a cryptography operation (col. 1, lines 50-54). Ugon does not disclose that the cryptography operation is based on DES algorithm; however, Examiner takes Official Notice that using DES algorithm, a standard for symmetric encryption, is well known in the art. It would have been obvious at the time of the invention was made to modify the Ugon device to use DES algorithm because it is a standard for symmetric encryption.

11. Claims 19 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ugon as applied to claims 15 and 18 above, and further in view of Qiu et al (6,804,782). Ugon does not disclose using a key that creates the complementary current variation. Qiu discloses using dummy operations to disguise power consumption and processor cycle time to prevent power attack and timing attack on cryptographic operations. Qiu further discloses using a key which triggers the dummy operations so as to result in a complementary current variation (Abstract; col. 1, lines 46-54; col. 2, lines 39-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Ugon to use using a key that creates the complementary current variation, as taught by Qiu. The motivation for doing so would have been to prevent both power and timing attacks simultaneously. Since frequency is calculated using the processor cycle time, inherently, reconstruction of consumption characteristics associated with the cryptographic operation using frequency is impeded.

12. Claims 2, 4, 7, 9 and 10-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patarin et al. (6,658,569) in view of Jahnich et al. (6,725,374).

Regarding claims 2 and 10, Patarin discloses a device comprising a central processing unit and one or more co-processors for performing cryptographic operations simultaneously and in parallel (Abstract; Fig. 2, step A; col. 12, lines 6-12 and 31-40). Patarin does not teach the use of dummy operations when performing a cryptographic operation. Jahnich discloses using dummy operations, whose execution does not

influence an encryption result and that the consumption characteristics generated by the dummy operation is part of the consumption characteristics of the smart card when executing the cryptographic operation and the dummy operation so that reconstruction of the consumption characteristics associated with performing the cryptographic operation is impeded (col. 6, lines 29-52). It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the method of Patarin to use dummy operations when performing a cryptographic operation, as taught by Jahnich. Accordingly, the dummy operation is performed in parallel and simultaneously with the cryptography operations.

Regarding claims 4, 7, 11-13, Patarin further discloses that the cryptographic operation is split up into at least two sub-operations and at least two processors perform the sub-operations in parallel and simultaneously, while subsequently corresponding sub-results are combined to an overall result of the overall cryptographic operation (Fig. 2; col. 12, lines 6-12 and 31-40).

Regarding claim 9, Patarin further discloses that the sub-operations are parts of an encryption in accordance with DES (figures 3a-b).

13. Claims 3, 6, 8 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patarin in view of Jahnich as applied to claims 2, 4, 7 and 13 above, and further in view of Tan (6,490,353).

Regarding claims 3 and 6, Patarin and Jahnich do not disclose that the selection of a processor to perform a cryptographic operation is randomly controlled. Tan

discloses that that the selection of a processor to perform a certain cryptographic operation is randomly controlled (col. 3, lines 60-64; col. 6, lines 6-12). It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the combined method of Patarin and Jahnich such that the selection of a processor to perform a cryptographic operation is randomly controlled, as taught by Tan, so that security could further be enhanced.

Regarding claims 8 and 14, Patarin and Jahnich do not disclose that the split-up of the cryptographic operation is randomly controlled. Tan discloses that data to be encrypted is segmented into blocks and that the size of each data block and length of the corresponding encryption key for each block are randomly selected (col. 3, lines 8-42); the selection of the block size and the key length meet the limitation of splitting up a cryptographic operation. It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the combined method of Patarin and Jahnich such that the split-up of the cryptographic operation is randomly controlled, as taught by Tan, to increase the degree of difficulty in attacking the encryption system.

14. Claims 15-18, 20-26 and 28 rejected under 35 U.S.C. 103(a) as being unpatentable over Patarin in view of Ohki et al (6,839,847).

Regarding claims 15-16, 18, 20, 22, 24 and 28, Patarin discloses a method of performing a cryptographic operation in a device, the device including at least two processors; the method comprising: performing a cryptographic operation in a first processor; performing a second operation in a second processor, the second operation

being performed simultaneously and in parallel with performing the cryptographic operation so that consumption characteristics of the device is a superimposition of consumption characteristics associated with performing the cryptographic operation and consumption characteristics associated with performing the second operation (Abstract; Fig. 2, step A; col. 12, lines 6-12 and 31-40). Patarin does not disclose that the second operation associated with consumption characteristics complementary to consumption characteristics associated with the cryptographic operation. Ohki discloses a device performing two operations: a cryptographic operation using normal input data and another operation using inverted input data, such that the power consumption of the device remains constant (col. 2, line 36 – col. 3, line 6), the Ohki operations meets the limitation that power consumption characteristics associated with one operation is complementary to that associated with the other. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Patarin method such that the power consumption characteristics associated with one operation is complementary to that associated with the other operation, as taught by Ohki, in order to reduce the correlation/dependency between data processing and the current consumption of an IC card.

Regarding claim 17, the claim limitation is interpreted as that the consumption characteristics associated with the cryptographic operation is concealed by the consumption characteristics of the device (see Specification, p. 5, line 32 – p. 6, line 5). Claim 17 is rejected on the same basis as claim 15 above.

Regarding claims 21 and 23, Patarin further discloses that the cryptographic operation is split up into at least two sub-operations and at least two processors perform the sub-operations in parallel and simultaneously, while subsequently corresponding sub-results are combined to an overall result of the overall cryptographic operation (Fig. 2; col. 12, lines 6-12 and 31-40).

15. Claims 19 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patarin and Ohki as applied to claims 15 and 18 above, and further in view of Qiu. Patarin and Ohki do not disclose using a key that creates the complementary current variation. Qiu discloses using dummy operations to disguise power consumption and processor cycle time to prevent power attack and timing attack on cryptographic operations. Qiu further discloses using a key which triggers the dummy operations so as to result in a complementary current variation (Abstract; col. 1, lines 46-54; col. 2, lines 39-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Patarin and Ohki to use using a key that creates the complementary current variation, as taught by Qiu. The motivation for doing so would have been to prevent both power and timing attacks simultaneously. Since frequency is calculated using the processor cycle time, inherently, reconstruction of consumption characteristics associated with the cryptographic operation using frequency is impeded.

16. Claims 25-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patarin and Ohki as applied to claims 15 above, and further in view of Tan. Patarin and Ohki do not disclose that the selection of a processor to perform a cryptographic operation is randomly controlled. Tan discloses that that the selection of a processor to perform a certain cryptographic operation is randomly controlled (col. 3, lines 60-64; col. 6, lines 6-12). It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the combined method of Patarin and Ohki such that the selection of a processor to perform a cryptographic operation is randomly controlled, as taught by Tan, so that security could further be enhanced.

Conclusion

17. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 6,327,661 to Kocher et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

9/26/05

GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100